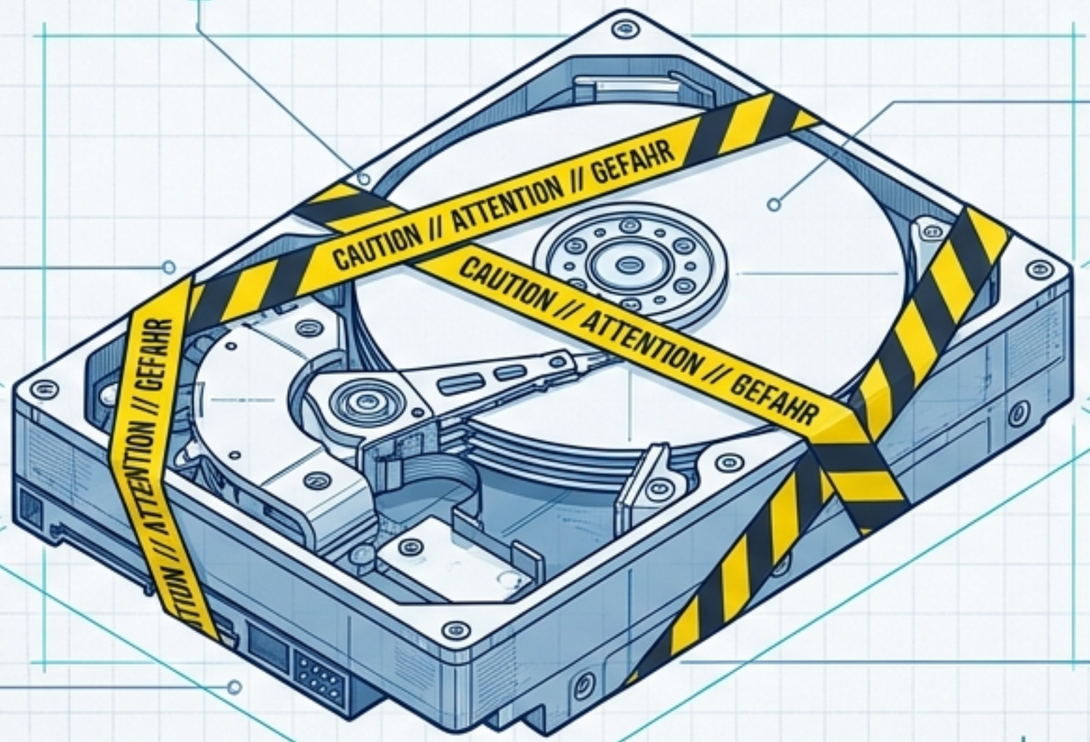
DOSSIER : MD-104-2014

STATUT : ACTIF

NIVEAU D'AUTORISATION : EXPERT

L'ANATOMIE D'UNE ENQUÊTE NUMÉRIQUE LÉGALE

Transformer le chaos numérique en preuves admissibles.



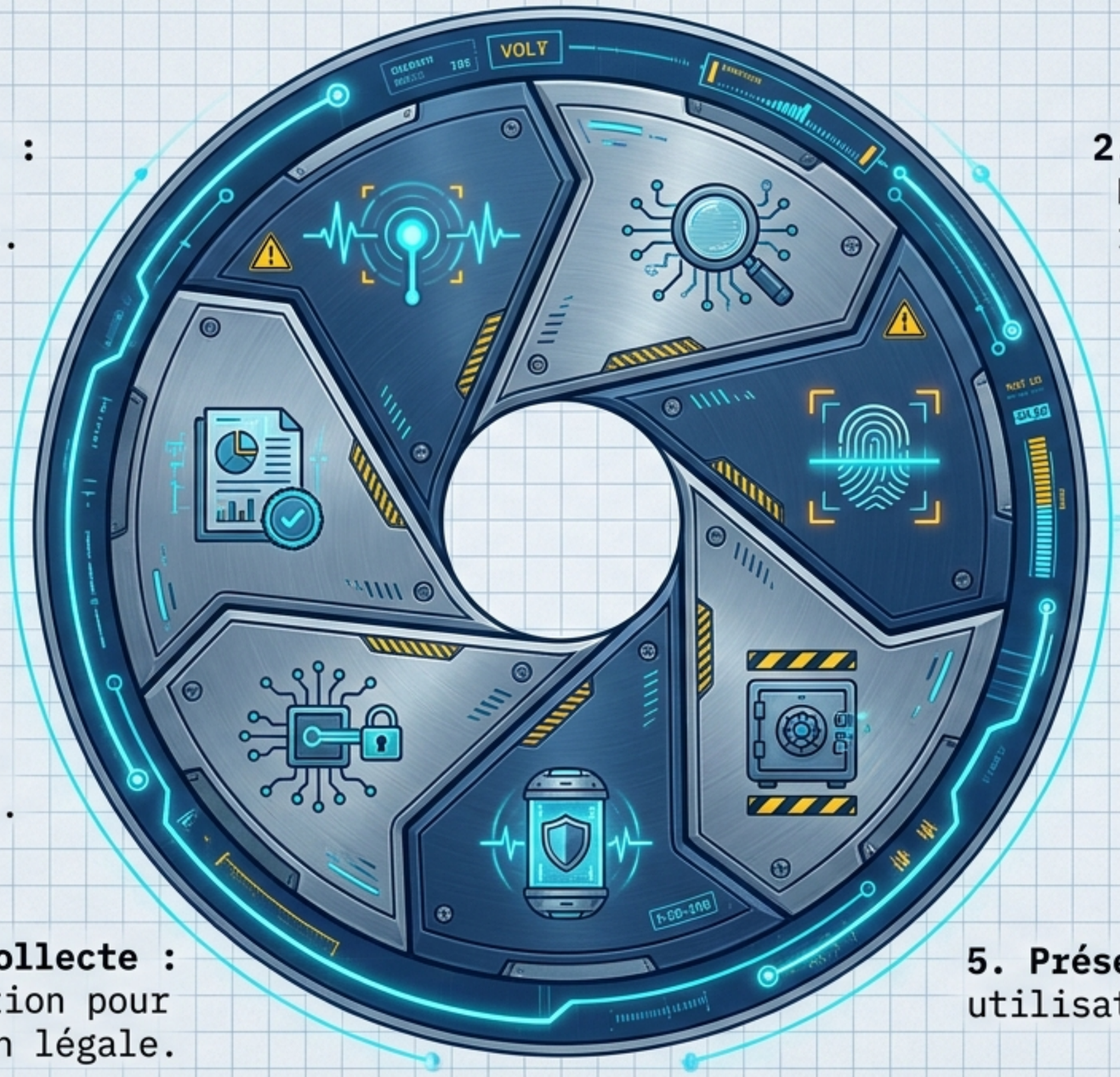
HORODATAGE : 2024-11-20

RÉFÉRENCE : PROTOCOLE D'INTERVENTION

Gemini Notebook

1. Détection : Confirmer l'incident.

2. Identification : Repérer les indices laissés.



3. Évaluation : Diagnostic préliminaire de la scène.

4. Perquisition : Saisie légale des artefacts.

5. Préservation pour utilisation légale.

5. Collecte : Préservation pour utilisation légale.

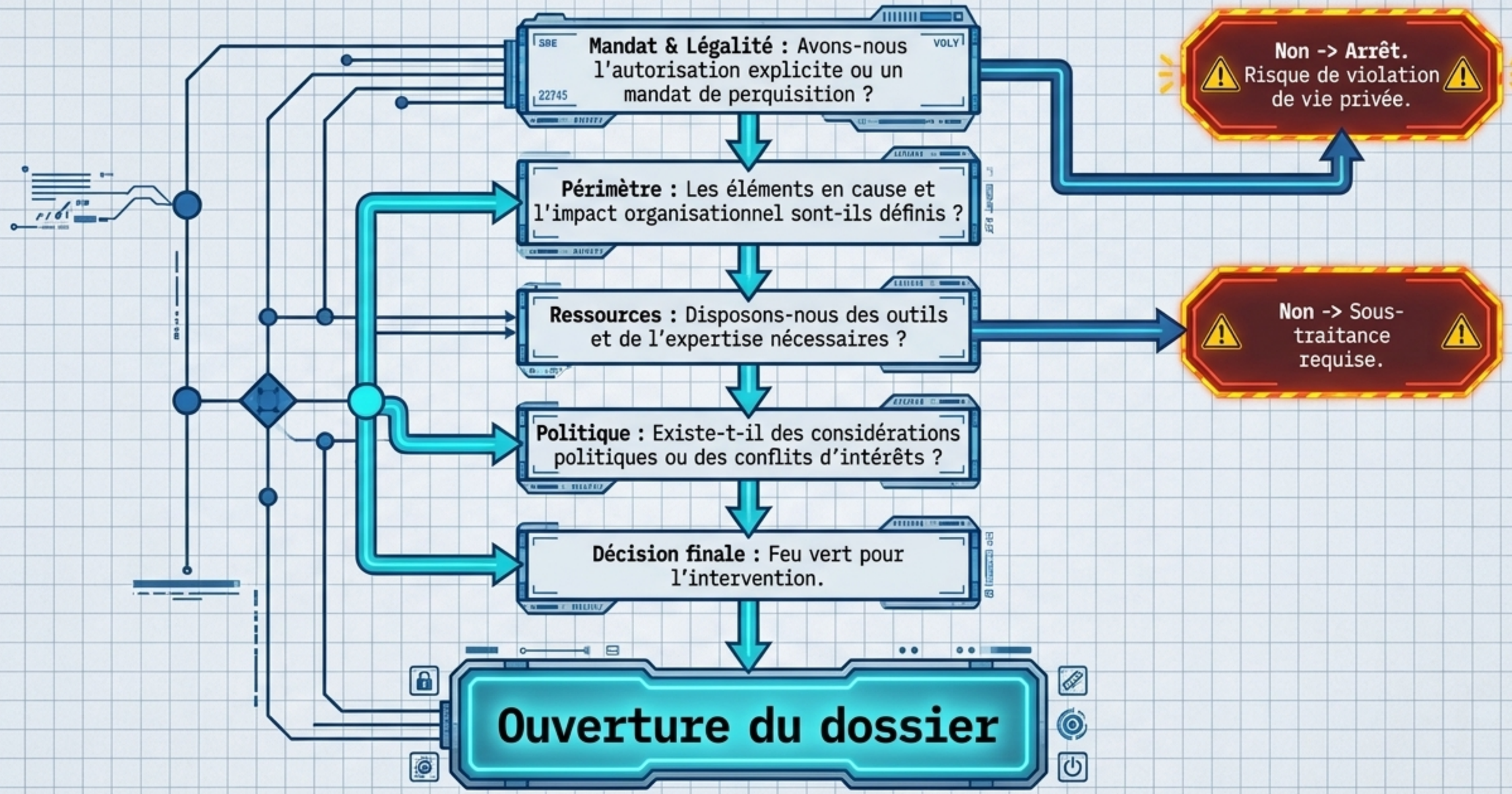
6. Clôture : Fin de l'implication active.

7. Rapport : Synthèse médico-légale.

Gemini Notebook

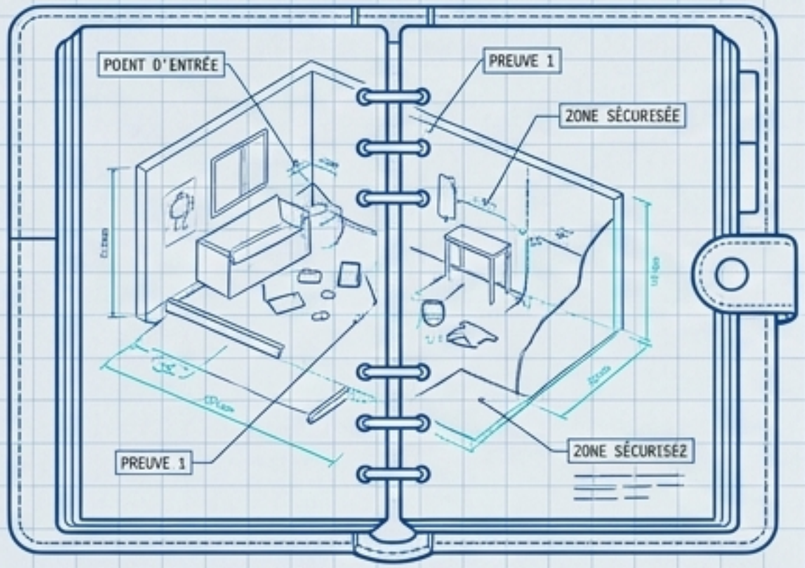
CASE ID: DD-2024-PROC-7 // **TIMESTAMP:** 2024-05-20 10:15:22 UTC // **CLASSIFICATION:** DECISION TREE LOGIC GATE // **AUTHORIZED BY:** J. DOE, LEAD INVESTIGATOR

FLOWCHART: GO/NO-GO DECISION TREE FOR INTERVENTION



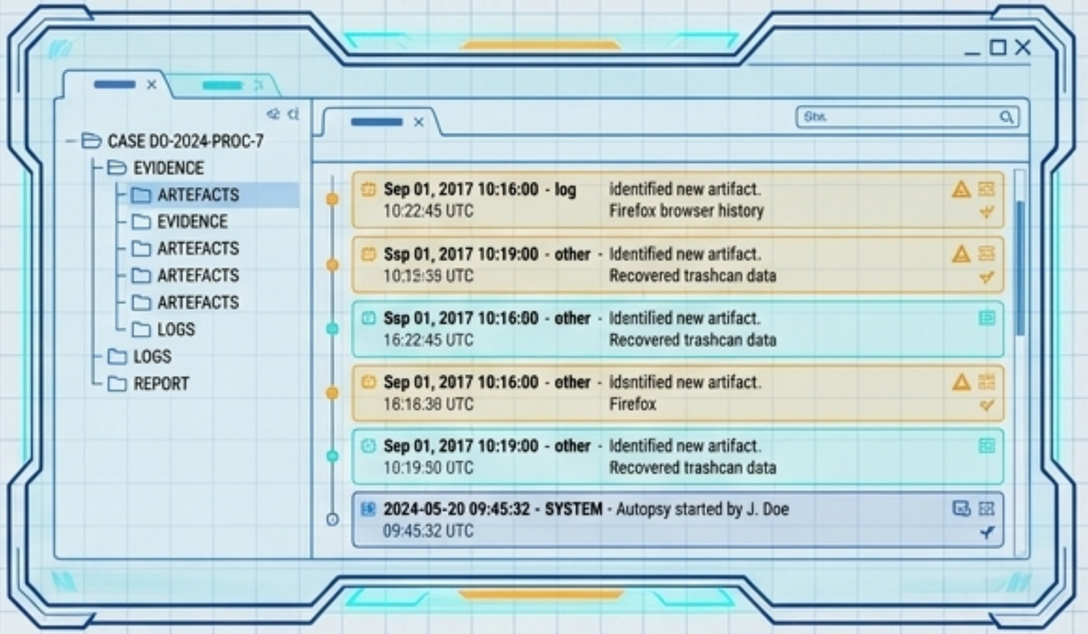
Gemini Notebook

CASE ID: DD-2024-PROC-7 // TIMESTAMP: 2024-05-20 10:22:45 UTC // CLASSIFICATION: ANALYTICAL EVIDENCE DOCUMENTATION // AUTHORIZED BY: J. DOE, LEAD INVESTIGATOR



Le Journal Papier

Essentiel pour les croquis de la scène, la documentation initiale, et la prise de notes immédiate avant le démarrage des systèmes.



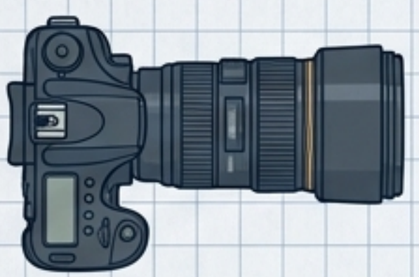
Le Journal Numérique (Autopsy)

Logiciel de gestion de cas (ex: Kali Linux). Assure l'immuabilité et la structuration en arborescence parent/enfant des artefacts analysés.

⚠ Données Obligatoires : Date, heure, lieu, personnes présentes, témoins, et classement de la volatilité des supports. ⚠

Gemini Notebook

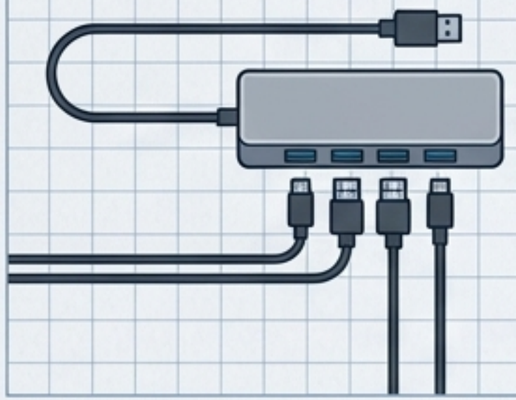
CASE ID: DD-2024-PROC-8 // TIMESTAMP: 2024-05-20 11:00:12 UTC // CLASSIFICATION: FIRST RESPONDER TACTICAL CHECKLIST // AUTHORIZED BY: J. DOE, LEAD INVESTIGATOR











Le Mandat du Premier Intervenant : Fixer la Scène.

1. **Isoler :** Délimiter la zone avec du ruban de signalisation. Aucune compromission physique.
2. **Documenter :** Photographier l'écran actif (sans ruban), les câbles connectés, et l'état général.
3. **Gérer les risques :** Évaluer les menaces (ex: effacement à distance) et identifier les témoins.

⚠ **La Trousse Tactique :** Appareil photo, Hub 4 ports (non commutateur), bloqueurs d'écriture matériels, formulaires de divulgation.

Gemini Notebook

CASE ID: DD-2024-PROC-9 // TIMESTAMP: 2024-05-20 11:30:00 UTC // CLASSIFICATION: MATRICE DES RESPONSABILITÉS // AUTHORIZED BY: J. DOE, LEAD INVESTIGATOR

Matrice des Responsabilités : confinement vs extraction

Premier Intervenant



Objectif : Préservation de l'état initial.

Action technique : Minime. Photographie des états d'alimentation.

Livrable : Scène sécurisée et inventaire préliminaire.

Expert en Criminalistique



Objectif : Extraction profonde et maintien de l'admissibilité.

Action technique : Création d'images bit à bit, hachage, analyse de la mémoire (dump RAM .raw).

Livrable : Chaîne de possession, rapport d'expertise, témoignage au tribunal.

⚠ Données Obligatoires : Cette matrice définit la séparation des rôles pour assurer l'intégrité de la preuve. ⚠

Gemini Notebook

CASE ID: DD-2024-PROC-10 // TIMESTAMP: 2024-05-20 12:00:00 UTC // CLASSIFICATION: DIAGNOSTIC POWER STATE COMPARISON // AUTHORIZED BY: J. DOE, LEAD INVESTIGATOR

Le Dilemme de l'Alimentation : Systèmes Actifs vs Éteints

Système Sous Tension (Live)



Risque : Modification du système par l'enquêteur ou malware actif.

Avantage : Accès aux **données volatiles** (mémoire RAM, processus, connexions réseau). Crucial pour les **malwares sans fichiers**.

Système Hors Tension (Dead)



Risque : **Perte irréversible** des clés de chiffrement en mémoire vive et des tables de routage.

Avantage : Arrêt immédiat de la destruction des données sur le disque. Possibilité de **clonage matériel sécurisé**.

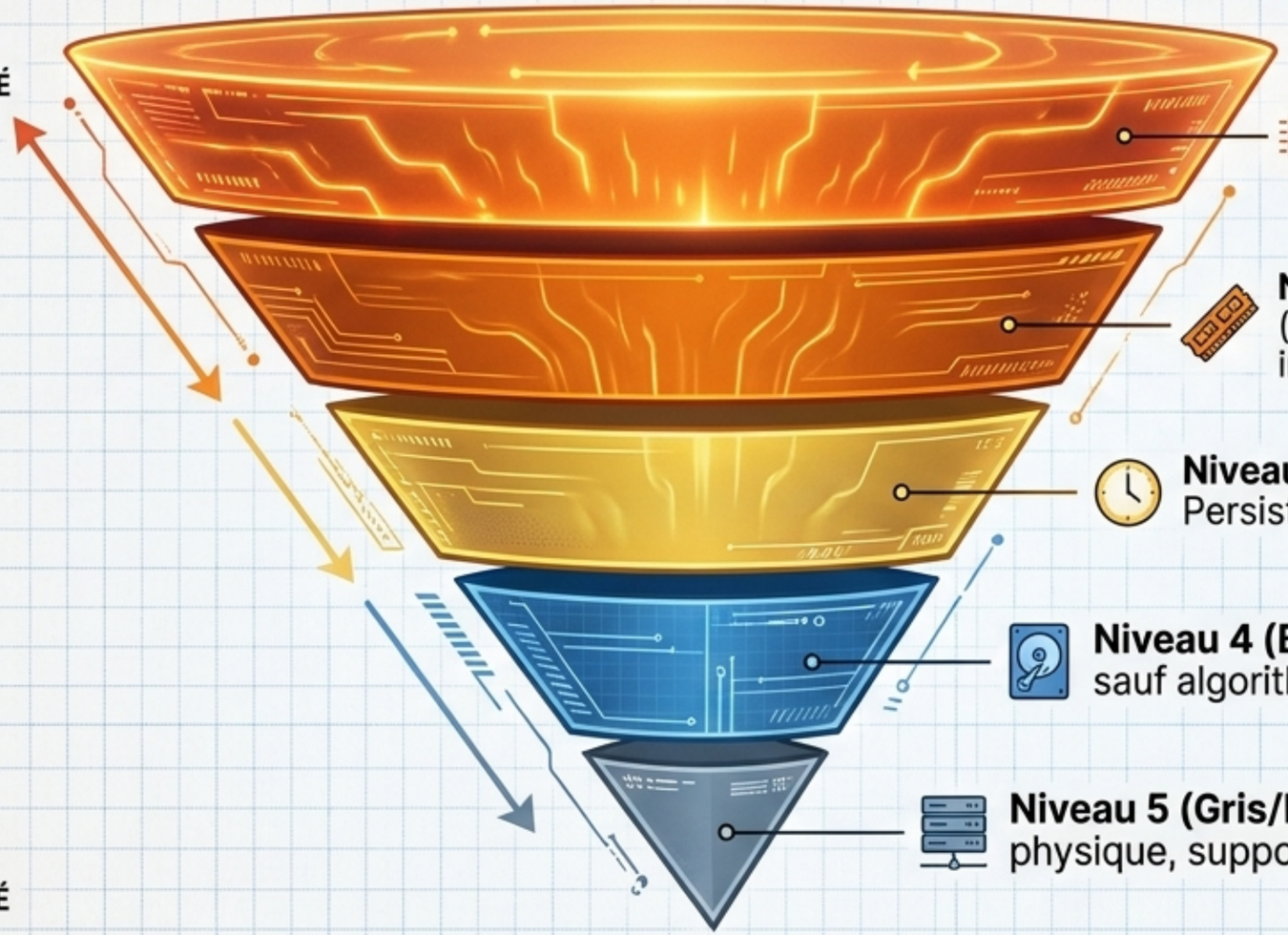
⚠ **Règle d'or** : Ne modifiez l'état d'alimentation qu'en cas de nécessité absolue et documentez chaque changement. ⚠

Gemini Notebook

Ordre de Volatilité : La Règle d'Extraction (RFC 3227)

CASE ID: DD-2024-PROC-11 // **TIMESTAMP:** 2024-05-20 13:00:00 UTC // **CLASSIFICATION:** ORDRE DE VOLATILITÉ (RFC 3227) // **AUTHORIZED BY:** J. DOE, LEAD INVESTIGATOR

HAUTE VOLATILITÉ



BASSE VOLATILITÉ

Niveau 1 (Rouge/Nanosecondes) : Caches du CPU, Registres. En constante évolution. Capture immédiate requise.

Niveau 2 (Orange/Millisecondes) : Mémoire vive (RAM), tables de routage, cache ARP. Perdues instantanément en cas de coupure de courant.

Niveau 3 (Jaune/Heures) : Fichiers temporaires. Persistance modérée.

Niveau 4 (Bleu / Stable) : Disques durs. Risque faible, sauf algorithmes TRIM (SSD).

Niveau 5 (Gris/Froid) : Journaux distants, topologie physique, supports d'archivage.

ATTENTION: L'ordre d'extraction doit strictement suivre la volatilité pour maximiser la récupération des preuves.

Gemini Notebook

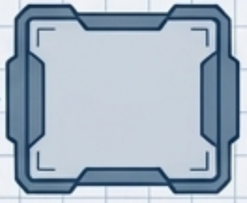
CASE ID: DD-2024-PROC-12 // TIMESTAMP: 2024-05-20 14:00:00 UTC // CLASSIFICATION: RÈGLE D'OR DE LA CRIMINALISTIQUE NUMÉRIQUE // AUTHORIZED BY: J. DOE, LEAD INVESTIGATOR

Ne jamais analyser l'appareil original. Toute modification est une contamination.

La Règle d'Or de la Criminalistique Numérique



ORIGINAL ISOLÉ



Étape 1 : Isoler.
Sécuriser le matériel original.

Étape 2 : Cloner.
Créer de multiples copies bit à bit parfaites.

Étape 3 : Valider (Hachage).
Calculer et comparer les empreintes cryptographiques (Hashes) de l'original et des copies pour prouver l'exactitude.

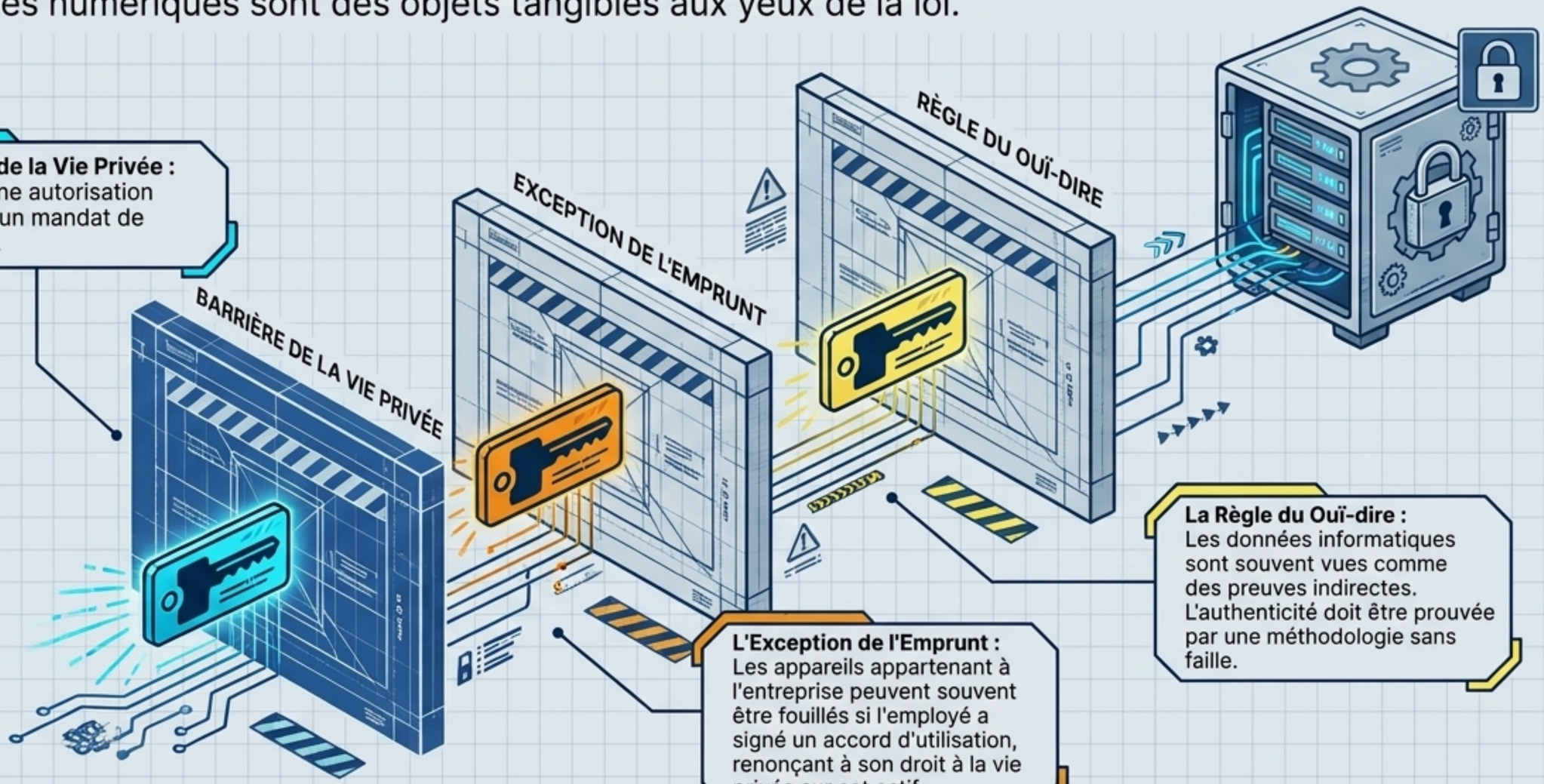
Étape 4 : Bloquer.
Activer la protection matérielle ou logicielle en écriture sur les clones.

Étape 5 : Analyser.
Procéder à l'investigation sur les copies protégées.

Gemini Notebook

Surmonter les Obstacles Juridiques (Perquisition et Saisie)

Les données numériques sont des objets tangibles aux yeux de la loi.



La Barrière de la Vie Privée : Nécessite une autorisation explicite ou un mandat de perquisition.

L'Exception de l'Emprunt : Les appareils appartenant à l'entreprise peuvent souvent être fouillés si l'employé a signé un accord d'utilisation, renonçant à son droit à la vie privée sur cet actif.

La Règle du Ouï-dire : Les données informatiques sont souvent vues comme des preuves indirectes. L'authenticité doit être prouvée par une méthodologie sans faille.

Confidentialité : Vue convimages loarvn this pre: usts snowing of ronoherrematle. Mevaraid sedleler that oiolau san permto les ono indoride locninds.dar: arice varty execedent.
Confidentialité : Nous abcurence dans the rest psezedent detnm seccion.arenoents oe resilied ot transnis in signé un comnandenta sangent anes imequet.

Gemini Notebook

METADATA | REDACTERS | REDATUCTED

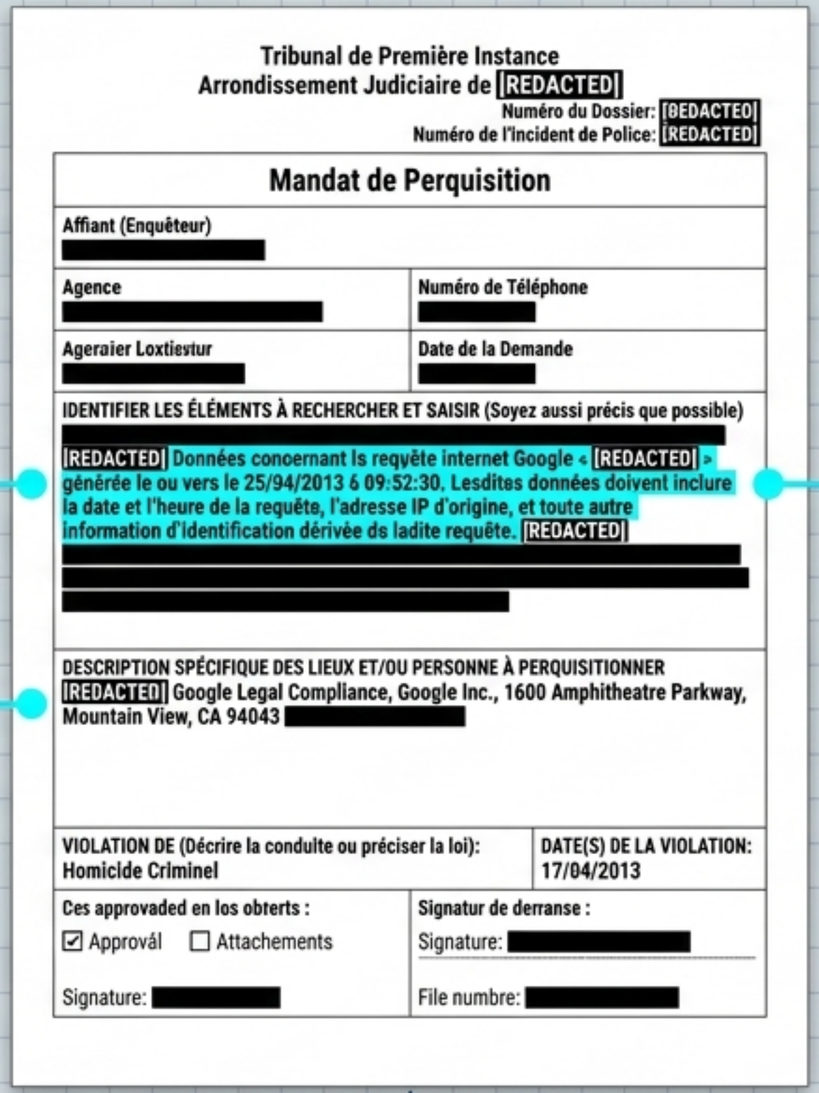
L'Anatomie d'un Mandat (La Précision Lexicale)

⚠️ 1. Cause Probable :

Doit s'appuyer sur des faits incontestables, pas des hypothèses (ex: une IP seule est souvent insuffisante).

⛔ 3. Le Périmètre de Saisie :

Si de nouvelles preuves non liées au mandat initial sont trouvées (ex: drogues vs. fraude), l'analyse doit cesser jusqu'à l'obtention d'un nouveau mandat étendu.



Tribunal de Première Instance
Arrondissement Judiciaire de [REDACTED]
Numéro du Dossier: [REDACTED]
Numéro de l'Incident de Police: [REDACTED]

Mandat de Perquisition

Affiant (Enquêteur) [redacted]

Agence [redacted] | Numéro de Téléphone [redacted]

Ageraier Loxtiestur [redacted] | Date de la Demande [redacted]

IDENTIFIER LES ÉLÉMENTS À RECHERCHER ET SAISIR (Soyez aussi précis que possible)

[REDACTED] Données concernant la reqvête internet Google « [REDACTED] » générée le ou vers le 25/94/2013 ó 09:52:30. Lesdites données doivent inclure la date et l'heure de la requête, l'adresse IP d'origine, et toute autre information d'identification dérivée ds ladite requête. [REDACTED]

DESCRIPTION SPÉCIFIQUE DES LIEUX ET/OU PERSONNE À PERQUISITIONNER

[REDACTED] Google Legal Compliance, Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 [redacted]

VIOLATION DE (Décrire la conduite ou préciser la loi): Homicide Criminel

DATE(S) DE LA VIOLATION: 17/04/2013

Ces approvaded en los obterts :
☑ Approvál ☐ Attachements
Signature: [redacted]

Signatur de derranse :
Signature: [redacted]
File numbre: [redacted]

🔍 2. Annotation Lexicale :

Le terme 'Pédopornographie' déclenche des lois fédérales sévères, tandis que 'Comportement sexuel explicite' peut n'enfreindre que le règlement interne. L'erreur de qualification invalide l'enquête.

CONFIDENTIAL: This document contains proprietary information. Unauthorized distribution is strictly prohibited.
Gemini Notebook

CASE ID: DD-2024-PROC-15 // **TIMESTAMP:** 2024-05-20 17:00:00 UTC // **CLASSIFICATION:** LA CHAÎNE DE POSSESSION // **AUTHORIZED BY:** J. DOE, LEAD INVESTIGATOR

La Chaîne de Possession (Cycle de Vie de la Preuve)

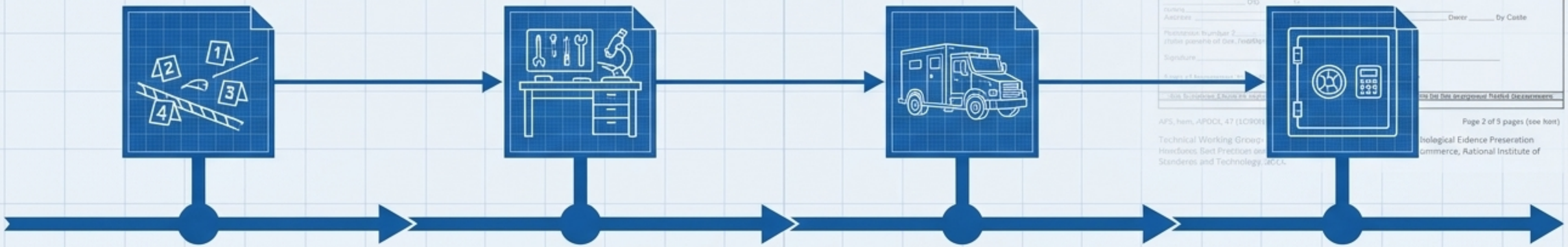
L'authenticité repose sur un registre ininterrompu.

T0 : État Initial. Documentation par le premier intervenant.

T1 : Extraction. Mise en sac et scellement par l'expert.

T2 : Transport. Mouvement tracé avec signataires.

T3 : Stockage. Dépôt en salle des scellés. Accès restreint et journalisé.



Avertissement : Une seule faille dans la documentation expose la preuve à l'inadmissibilité pour contamination extérieure.

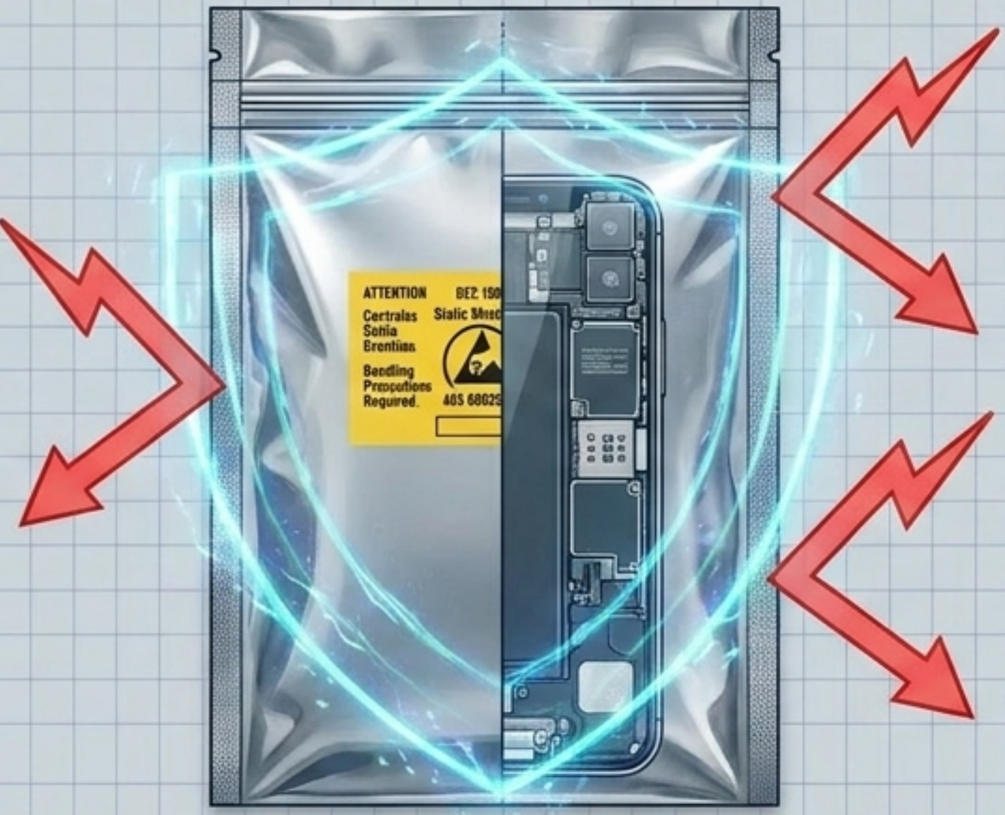
Gemini Notebook

CASE ID: DD-2024-PROC-16 // TIMESTAMP: 2024-05-20 17:00:00 UTC // CLASSIFICATION: PRÉSERVATION PHYSIQUE // AUTHORIZED BY: J. DOE, LEAD INVESTIGATOR

Préservation Physique : Contre les Menaces Invisibles

Décharge Électrostatique (ESD) :

Les sacs de protection (ex: normes MIL-STD-3010) empêchent l'accumulation statique qui détruit les puces.



Communications Sans Fil (Wipe à distance) :

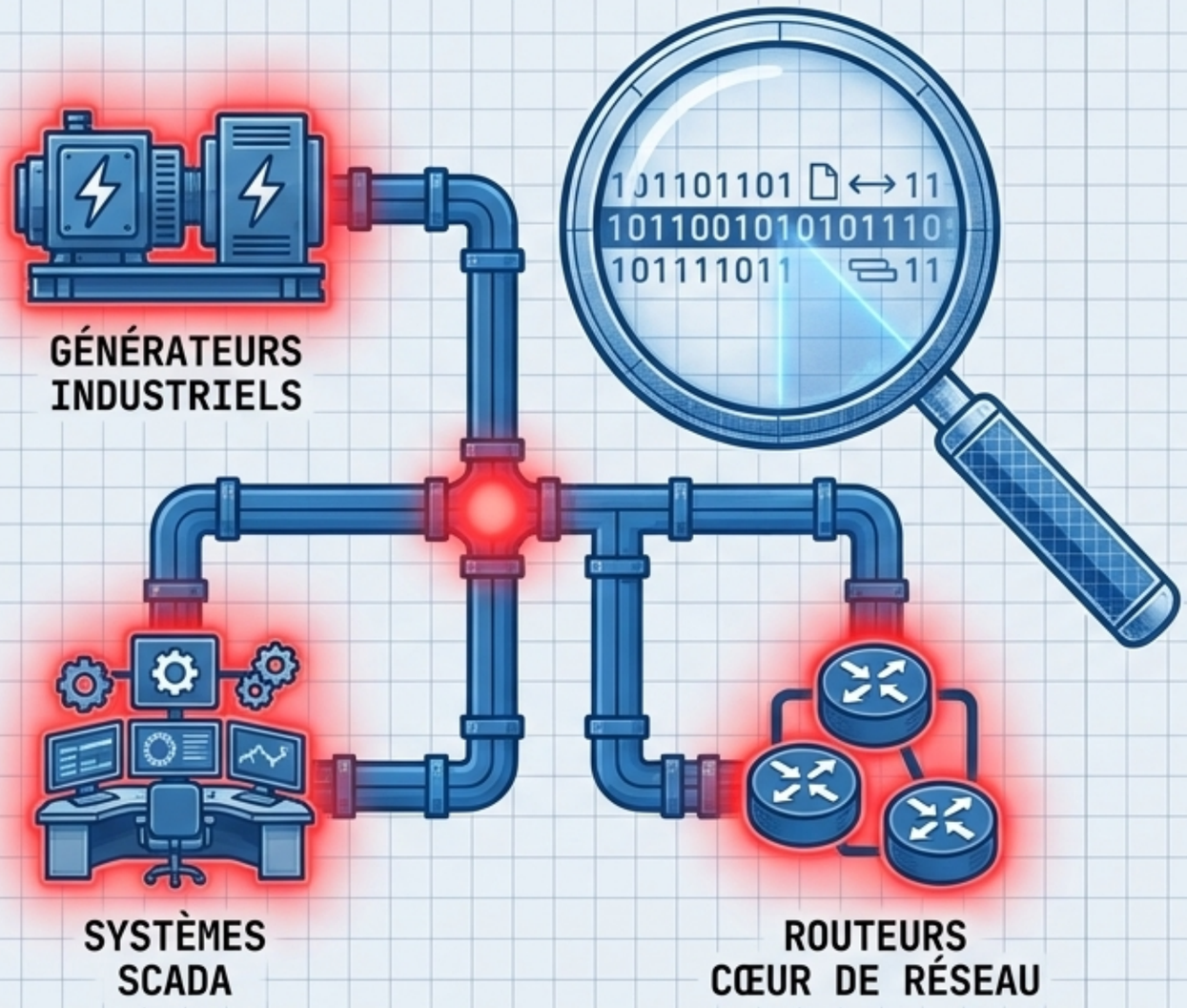
Les sacs intégrant une cage de Faraday bloquent les ondes cellulaires, Wi-Fi et Bluetooth pour les mobiles et objets connectés.

Surchauffe Thermique :

Les appareils laissés sous tension dans des contenants hermétiques nécessitent parfois des glacières pour éviter la fusion des composants matériels.

CASE ID: DD-2024-PROC-14 // TIMESTAMP: 2024-05-20 16:00:00 UTC // CLASSIFICATION: L'ANATOMIE D'UN MANDAT // MUSIS

CONFIDENTIAL: This document contains proprietary information. Unauthorized distribution is strictly prohibited.
Gemini Notebook



CRITICAL UPTIME: NE PAS ARRÊTER.

CAS SPÉCIAL : INFRASTRUCTURES CRITIQUES ET RÉSEAUX ACTIFS

Comment enquêter quand l'arrêt du système paralyserait l'entreprise (ex: systèmes SCADA, routeurs vitaux) ?

L'APPROCHE NON DESTRUCTIVE :

Impossible d'isoler physiquement le disque. L'investigation s'effectue sur les empreintes du réseau.

TECHNIQUES :

Capture de trafic en temps réel, extraction de journaux historiques, analyse des paquets sans interruption de service.

CONFIDENTIAL: This document contains proprietary information. Unauthorized distribution is strictly prohibited.

Gemini Notebook

Synthèse : L'Équation de l'Admissibilité

[Intégrité Technique] + **[Rigueur Procédurale]** = **PREUVE ADMISSIBLE**



Copies bit à bit,
Hachage cryptographique validé,
Bloqueurs d'écriture matériels.
(Prouve que la donnée est intacte).



Mandats précis respectés,
Chaîne de possession continue,
Registres d'accès immuables.
(Prouve que l'obtention est légale).



Conclusion : Si une seule variable échoue (hachage altéré OU vice de forme du mandat), l'intégralité de l'enquête est nulle et non avenue devant un tribunal. L'excellence technique ne compense jamais une erreur légale.

CONFIDENTIAL: This document contains proprietary information. Unauthorized distribution is strictly prohibited.

Gemini Notebook